

Claims

[c1] A method for establishing a secure communication channel between a client and an application server, the method comprising the steps of:

- (a) obtaining, by a web server, a MIME type document and a ticket associated with a client, the MIME type document comprising a client application program, the ticket having an identifier and a session key;
- (b) receiving, by a web browser, the MIME type document and the ticket from the web server;
- (c) invoking, by the web browser, the received client application program;
- (d) establishing an application communication channel between the client and the application server;
- (e) transmitting, by the client application program, the identifier from the ticket to the application server over the application communication channel;
- (f) obtaining, by the application server, a copy of the session key from the web server using the identifier; and
- (g) encrypting communications between the client application program and the application server over the application communication channel using the session key.

- [c2] The method of claim 1 wherein step (a) further consists of establishing a secure web communication channel between the web browser and the web server.
- [c3] The method of claim 1 wherein step (c) further consists of transferring, by the web browser, the ticket to the client application program.
- [c4] The method of claim 1 wherein step (g) further comprises decrypting communications between the client application program and the application server using the session key.
- [c5] The method of claim 1 wherein step (a) further comprises receiving, at the web server, a request from the client to have an application program executed on the application server and to have output from the application program executing on the application server transmitted to the client application program.
- [c6] The method of claim 5 wherein step (g) further comprises executing, by the application server, the application program identified in the request, and transmitting, by the application server, the output of the application program over the application communication channel via a remote display protocol.
- [c7] The method of claim 1 wherein step (a) further com-

prises obtaining a MIME type document having a remote display client for the client application program.

- [c8] The method of claim 1 wherein step (c) further comprises installing the client application program for a first time on the client.
- [c9] The method of claim 1 wherein step (a) further comprises obtaining a ticket having an application server certificate for the identifier.
- [c10] The method of claim 1 wherein step (a) further comprises obtaining a ticket having a session key substantially equivalent to a null value.
- [c11] The method of claim 1 wherein step (a) further comprises obtaining a ticket granting access for a single use.
- [c12] The method of claim 1 wherein step (a) further comprises obtaining a ticket granting access to a previously authorized resource.
- [c13] The method of claim 1 wherein step (e) further comprises transmitting a password to the application server.
- [c14] The method of claim 1 wherein step (a) further comprises obtaining the MIME type document from the application server.

- [c15] The method of claim 6 wherein step (g) further comprises using the Independent Computing Architecture protocol for the remote display protocol.
- [c16] The method of claim 6 wherein step (g) further comprises using the Remote Display Protocol for the remote display protocol.
- [c17] A client system for establishing a secure communication channel with an application server, the client system comprising:
 - a web browser associated with a client;
 - a web server in communication with the web browser over a web communication channel, the web server obtaining a MIME type document and a ticket associated with the client, the MIME type document comprising a client application program, the ticket having an identifier and a session key;
 - the web browser receiving, from the web server, the ticket and the MIME type document,
 - the web browser invoking the received client application program;
 - an application server, in communication with the client over an application communication channel, receiving the identifier from the client application program, and the application server, in communication with the web server, obtaining a copy of the session key by using the

identifier; and
the application server and the client application program
encrypting communications over the application com-
munication channel using the session key.

- [c18] The system of claim 17 wherein the web communication channel is secure.
- [c19] The system of claim 17 wherein the web browser transfers the ticket to the client application program.
- [c20] The system of claim 17 wherein the application server and the client application program decrypt communications over the application communication channel using the session key.
- [c21] The system of claim 17 wherein the web server receives a request from the client to have an application program executed on the application server and to have output from the application program executing on the application server transmitted to the client application program.
- [c22] The system of claim 21 wherein the application server executes the application program identified in the request, and transmits the output of the application program to the client application program over the application communication channel via a remote display protocol.

- [c23] The system of claim 17 wherein the client application program is a remote display client.
- [c24] The system of claim 17 wherein the client application program is installed for a first time on the client.
- [c25] The system of claim 17 wherein the identifier is an application server certificate.
- [c26] The system of claim 17 wherein the session key is substantially equivalent to a null value.
- [c27] The system of claim 17 wherein the ticket grants access for a single use.
- [c28] The system of claim 17 wherein the ticket grants access to a previously authorized resource.
- [c29] The system of claim 17 wherein the client transmits a password to the application server.
- [c30] The system of claim 17 wherein the web server obtains the MIME type document from the application server.
- [c31] The system of claim 22 wherein the remote display protocol is the Independent Computing Architecture protocol.
- [c32] The system of claim 22 wherein the remote display pro-

tocol is the Remote Display Protocol.

- [c33] A method for establishing a secure communication channel with an application server, the method comprising the steps of:
 - (a) receiving a MIME type document and a ticket from the web server, the ticket having an identifier and a session key, and the MIME type document comprising a client application program;
 - (b) invoking the received client application program;
 - (c) establishing an application communication channel with an application server;
 - (d) transmitting the identifier from the ticket to the application server over the application communication channel to provide the application server with information for obtaining a copy of the session key; and
 - (e) encrypting communications to the application server over the application communication channel using the session key.
- [c34] The method of claim 33 wherein step (e) further comprises decrypting communications from the application server using the session key.
- [c35] The method of claim 33 wherein step (a) further comprises establishing a secure web communication channel between a web browser and the web server.

- [c36] The method of claim 35 wherein step (g) further comprises transferring the ticket from the web browser to the client application program.
- [c37] The method of claim 33 wherein step (a) further comprises sending, to the web server, a request to have an application program executed on the application server and to receive output from the application program executing on the application server.
- [c38] The method of claim 37 wherein step (e) further comprises executing, by the application server, the application program identified in the request, and transmitting, by the application server, the output of the application program over the application communication channel via a remote display protocol.
- [c39] The method of claim 33 wherein step (e) further comprises obtaining a MIME type document having a remote display client for the client application program.
- [c40] The method of claim 33 wherein step (a) further comprises installing the client application program for a first time.
- [c41] The method of claim 33 wherein step (a) further comprises obtaining a ticket having an application server

certificate for the identifier.

- [c42] The method of claim 33 wherein step (a) further comprises obtaining a ticket having a session key substantially equivalent to a null value.
- [c43] The method of claim 33 wherein step (a) further comprises obtaining a ticket granting access for a single use.
- [c44] The method of claim 33 wherein step (a) further comprises obtaining a ticket granting access to a previously authorized resource.
- [c45] The method of claim 33 wherein step (d) further comprises transmitting a password to the application server.
- [c46] The method of claim 38 wherein step (e) further comprises using the Independent Computing Architecture protocol for the remote display protocol.
- [c47] The method of claim 38 wherein step (e) further comprises using the Remote Display Protocol for the remote display protocol.
- [c48] A client system for establishing a secure communication channel with a client, the client system comprising:
a web browser in communication with a web server over a web communication channel, the web browser receiving, from the web server, a MIME type document and a

ticket, the MIME type document comprising a client application program, the ticket having an identifier and a session key;
a client application program invoked by the web browser; and
the client application program establishing an application communication channel with the application server, the client application program transmitting the identifier over the application communication channel, and the client application program encrypting communications to the application server over the application communication channel using the session key.

- [c49] The system of claim 48 wherein the client application program decrypts communications from the application server over the application communication channel using the session key.
- [c50] The system of claim 48 wherein the web browser transfers the ticket to the client application program.
- [c51] The system of claim 48 wherein the web browser transmits a request to have an application program executed on the application server and to have output of the application program executing on the application server transmitted to the client application program.

- [c52] The system of claim 51 wherein the application server executes the application program identified in the request, and transmits the output of the application program to the client application program over the application communication channel via a remote display protocol.
- [c53] The system of claim 48 wherein the client application program is a remote display client.
- [c54] The system of claim 48 wherein the client application program is installed for a first time on the client.
- [c55] The system of claim 48 wherein the identifier is an application server certificate.
- [c56] The system of claim 48 wherein the session key is substantially equivalent to a null value.
- [c57] The system of claim 48 wherein the ticket grants access for a single use.
- [c58] The system of claim 48 wherein the ticket grants access to a previously authorized resource.
- [c59] The system of claim 52 wherein the remote display protocol is the Independent Computing Architecture protocol.

[c60] The system of claim 52 wherein the remote display protocol is the Remote Display Protocol.

[c61] A method for establishing a secure communication channel with a client, the method comprising the steps of:

- (a) obtaining, by a web server, a MIME type document and a ticket associated with a client, the MIME type document comprising a client application program, the ticket having an identifier and a session key;
- (b) transmitting, by the web server, the MIME type document and the ticket to a web browser over a web communication channel;
- (c) invoking, by the web browser, the received client application program;
- (d) establishing an application communication channel with the client;
- (e) receiving, from the client application program, the identifier from the ticket over the application communication channel;
- (f) obtaining a copy of the session key from the web server using the identifier; and
- (g) encrypting communications to the client application program over the application communication channel using the session key.

- [c62] The method of claim 61 wherein step (g) further comprises decrypting communications from the client application program using the session key.
- [c63] The method of claim 61 wherein step (b) further comprises establishing a secure web communication channel between a web browser and the web server.
- [c64] The method of claim 63 wherein step (b) further comprises transferring, by the web browser, the ticket to the client application program.
- [c65] The method of claim 61 wherein step (a) further comprises receiving, at the web server, a request from the client to have an application program executed on the client's behalf and to have output from the application program, as it is executing, transmitted to the client application program.
- [c66] The method of claim 65 wherein step (g) further comprises executing the application program identified in the request, and transmitting the output of the application program over the application communication channel via a remote display protocol.
- [c67] The method of claim 61 wherein step (g) further comprises using a remote display client for the client application program.

- [c68] The method of claim 61 wherein step (e) further comprises installing the client application program for a first time on the client.
- [c69] The method of claim 61 wherein step (a) further comprises obtaining a ticket having an application server certificate for an identifier.
- [c70] The method of claim 61 wherein step (b) further comprises obtaining a ticket having a session key substantially equivalent to a null value.
- [c71] The method of claim 61 wherein step (a) further comprises obtaining a ticket granting access for a single use.
- [c72] The method of claim 61 wherein step (a) further comprises obtaining a ticket granting access to a previously authorized resource.
- [c73] The method of claim 61 wherein step (e) further comprises receiving a password from the client.
- [c74] The method of claim 61 wherein step (a) further comprises obtaining the MIME type document from an application server.
- [c75] The method of claim 66 wherein step (g) further comprises using the Independent Computing Architecture

protocol for the remote display protocol.

- [c76] The method of claim 66 wherein step (g) further comprises using the Remote Display Protocol for the remote display protocol.
- [c77] A server system for establishing a secure communication channel with a client, the server system comprising:
 - a ticket service generating a ticket associated with a client, the ticket having an identifier and a session key;
 - a web server in communication with the ticket service, the web server transmitting a MIME type document and the ticket to the client over a web communication channel, the MIME type document comprising a client application program; and
 - an application server receiving the identifier from the ticket from the client, obtaining a copy of the session key from the web server, establishing an application communication channel with the client, and encrypting communications to the client over the application communication channel using the session key.
- [c78] The system of claim 77 wherein the application server decrypts communications from the client over the application communication channel using the session key.
- [c79] The system of claim 77 wherein the web server receives

a request from the client to have an application program executed on the client's behalf and to have output from the application program, as it is executing, transmitted to the client.

- [c80] The system of claim 77 wherein the application server executes the application program identified in the request, and transmits the output of the application program to the client application program over the application communication channel via a remote display protocol.
- [c81] The system of claim 77 wherein the client application program is a remote display client.
- [c82] The system of claim 77 wherein the client application program is installed for a first time on the client.
- [c83] The system of claim 77 wherein the identifier is an application server certificate.
- [c84] The system of claim 77 wherein the session key is substantially equivalent to a null value.
- [c85] The system of claim 77 wherein the ticket grants access for a single use.
- [c86] The system of claim 77 wherein the ticket grants access to a previously authorized resource.

- [c87] The system of claim 77 wherein the application server receives a password from the client.
- [c88] The system of claim 77 wherein the web server obtains the MIME type document from the application server.
- [c89] The system of claim 80 wherein the remote display protocol is the Independent Computing Architecture protocol.
- [c90] The system of claim 80 wherein the remote display protocol is the Remote Display Protocol.